Journal of Number Theory **76**, 130–146 (1999)
Article ID jnth.1998.2339, available online at http://www.idealibrary.com on IDEAL®

Application de la méthode de Dem'janenko–Manin à certaines familles de courbes de genre 2 et 3

Leopoldo Kulesz

UFR de Mathématiques, Université Paris 7, 2, Place Jussieu, F-75251 Paris Cedex 05, France
E-mail: kulesz@math.jussieu.fr

et

Instituto de Desarollo Humano, Universidad Nacional de General Sarmiento, Roca 850 San Miguel Pcia. de Buenos Aires, 1663 Argentina
E-mail: lkulesz@ungs.edu.ar

Communicated by Yu. I. Manin

Received June 12. 1998

Q, qui admettent deux morphismes indépendants vers une courbe elliptique de rang 1 sur **Q**. La méthode de Dem'janenko–Manin peut donc s'appliquer et elle nous permettra de déterminer complètement l'ensemble des points rationnels de toutes les courbes des familles considérées. © 1999 Academic Press

We give examples of families of curves of genus 2 and 3 defined over **Q** with two independent morphisms to an elliptic curve of rank 1 over **Q**. The method of Dem'janenko–Manin may be applied and it will allow us to determine completely the set of rational points of any curve in the families that we consider. © 1999 Academic Press

INTRODUCTION

La conjecture de Mordell, démontrée par G. Faltings en 1983 [Fal1], établit qu'une courbe de genre $\geqslant 2$ définie sur un corps de nombres **K** possède au plus un nombre fini de points **K**-rationnels. Malheureusement, tant la preuve de Faltings que ses postérieures simplifications [Bom, Fal2, Voj] ne sont pas effectives, dans le sens où elles ne donnent pas une borne explicite de la hauteur des points rationnels. La détermination de tous les points rationnels d'une courbe donnée reste donc un problème difficile et, mis à part les arguments triviaux de localisation, seulement deux méthodes se sont montrées efficaces pour l'attaquer. Elles sont dues respectivement à C. Chabauty [Cha] (rendue effective par R. F. Coleman [Col]) et à V. Dem'janenko [Dem] (généralisée par Y. Manin [Man]). Ces méthodes s'appliquent à des familles particulières de courbes: celle de Chabauty, aux courbes de genre g dont la jacobienne est de rang $<g$ sur **K**, et celle de Dem'janenko–Manin, aux courbes qui admettent m morphismes indépendants vers une courbe elliptique de rang $<m$ sur **K**.

0022-314X/99 $30.00

Les exemples d'application de la méthode de Chabauty sont nombreux, nous pouvons citer par exemple [G-G, Col, Flyn, F-P-S, Bru, Wet]. Il n'en est pas de même pour la méthode de Dem'janenko–Manin; nous connaissons les résultats de Dem'janenko [Dem] améliorés par J. Silverman [Sil1] et G. Grigorov et N. Rizov [G-R] concernant entre autres, les familles de courbes $\mathscr{C}_b$ de genre 3 d'équation $x^4+y^4=bz^4$ (pour $b\in\mathbf{Z}$ tel que la courbe elliptique d'équation $y^2=x^3-bx$ soit de rang 1 sur le corps de nombres considéré).

Dans ce travail, nous nous proposons d'appliquer la méthode de Dem'janenko–Manin aux familles

$$\mathscr{F}=\{\mathscr{C}_a\colon ay^2=6(x^2-4)(x^2+2)(x^2+8);$$
$$a\in\mathbf{Z}_{>0} \text{ et } \mathscr{E}_{a^2}\colon y^2=x^3-a^2x \text{ est de rang 1 sur } \mathbf{Q}\},$$
$$\mathscr{G}=\{\mathscr{D}_a\colon ay^2=-x(x-1)(x+1)(x+2)(2x+1)(1+x+x^2)$$
$$a\in\mathbf{Z}_{>0} \text{ et } \mathscr{E}_{a^2}\colon y^2=x^3-a^2x \text{ est de rang 1 sur } \mathbf{Q}\},$$

pour montrer le résultat suivant:

THÉORÈME. *Soit $\mathscr{C}_a\in\mathscr{F}$ et $\mathscr{D}_a\in\mathscr{G}$. Alors,*

$$\begin{cases}\mathscr{C}_a(\mathbf{Q})=\{(\pm2,0)\} & \text{si } a\neq 6,\\ \mathscr{C}_6(\mathbf{Q})=\{(\pm2,0),(\pm4,\pm72),\pm\infty\},\\ \mathscr{D}_a(\mathbf{Q})=\{(0,0),(1,0),(-1,0),(-2,0),(-1/2,0)\}.\end{cases}$$

Je tiens à remercier Joseph Silverman, Bjorn Poonen et Grigor Grigorov pour l'attention qu'ils ont bien voulu porter à ce travail.

NOTATION

- Nous allons travailler dans le corps $\mathbf{Q}$ des nombres rationnels, même si toutes les démonstrations restent valables en remplaçant $\mathbf{Q}$ par un corps de nombres quelconque.
- Si $\mathscr{C}$ est une courbe algébrique définie sur $\mathbf{Q}$, $\mathscr{C}(\mathbf{Q})$ désigne l'ensemble de points de $\mathscr{C}$ à coordonnées dans $\mathbf{Q}$ et $\mathscr{J}(\mathscr{C})$ la jacobienne de $\mathscr{C}$.

• Si $\mathscr{E}$ est une courbe elliptique définie sur $\mathbf{Q}$, $\mathrm{Tors}(\mathscr{E}(\mathbf{Q}))$ désigne le sous-groupe de torsion de $\mathscr{E}(\mathbf{Q})$, et si $n \in \mathbf{Z}\backslash\{0\}$ et $P \in \mathscr{E}(\mathbf{Q})$,

$$[n]: \mathscr{E} \to \mathscr{E}$$

$$P \mapsto \underbrace{P + \cdots + P}_{n \text{ fois}}$$

désigne la multiplication par n dans $\mathscr{E}$.

• $d(\phi)$ désigne le degré du morphisme ϕ.

• H, la hauteur absolue sur $\bar{\mathbf{Q}}$.

• h, la hauteur absolue logarithmique sur $\bar{\mathbf{Q}}$.

• $\hat{h}$, la hauteur canonique sur $\mathscr{E}(\bar{\mathbf{Q}})$.

• Si $P = (x, y) \in \mathbf{Q}^2$ est un point rationnel du plan affine, nous allons considérer $h(P) = \max(|\text{numérateur}(x)|, |\text{dénominateur}(x)|)$.

1. PRÉLIMINAIRES

1.1. *La méthode de Dem'janenko–Manin*

Soient $\mathscr{C}$ une courbe projective non singulière sur $\mathbf{Q}$, $\mathscr{E}$ une courbe elliptique sur $\mathbf{Q}$ et $\phi_1, ..., \phi_l$ des morphismes de $\mathscr{C}$ dans $\mathscr{E}$ définis sur $\mathbf{Q}$.

DÉFINITION. Soit $P_0 \in \mathscr{C}(\mathbf{Q})$, posons $\bar{\phi}_i = \phi_i - \phi_i(P_0)$, $i = 1, ..., l$. Nous dirons que $\phi_1, ..., \phi_l$ sont indépendants sur $\mathbf{Q}$, si

$$\sum_{i=1}^{l} n_i \bar{\phi}_i = 0 \Rightarrow n_i = 0 \qquad \forall i = 1, ..., l.$$

Nous avons le résultat suivant [Dem, Cas, Serre]:

THÉORÈME. *Si $\phi_1, ..., \phi_l$ sont indépendants sur $\mathbf{Q}$ et $l > \mathrm{rang}_{\mathbf{Q}}(\mathscr{E})$, alors $\mathscr{C}(\mathbf{Q})$ est fini et peut être déterminé de manière effective.*

Dans cet article, nous allons appliquer la méthode de Dem'janenko–Manin au cas où $\mathbf{K} = \mathbf{Q}$ et $\mathrm{rang}_{\mathbf{Q}}(\mathscr{E}) = 1$.

Soit donc $\mathscr{E}$ une courbe elliptique de rang 1 sur $\mathbf{Q}$ et soit R un générateur de la partie libre de $\mathscr{E}(\mathbf{Q})$. Soit $\mathscr{C}$ une courbe de genre $\geqslant 2$, nous allons supposer qu'il existe deux morphismes ϕ_1 et ϕ_2: $\mathscr{C} \mapsto \mathscr{E}$, indépendants sur $\mathbf{Q}$ et tels que $d(\phi_1) = d(\phi_2) = d$.

Pour tout $P \in \mathscr{C}(\mathbf{Q})$, il existe par construction, des entiers n et m et des points T_1, T_2 dans $\mathrm{Tors}(\mathscr{E}(\mathbf{Q}))$ tels que:

$$\begin{cases} \phi_1(P) = [n]\, R + T_1 \\ \phi_2(P) = [m]\, R + T_2. \end{cases}$$

Par ailleurs, comme $\mathrm{Card}(\mathrm{Tors}(\mathscr{E}(\mathbf{Q}))) \leqslant 16$ [Maz], il existe $u \in \mathbf{Z}\backslash\{0\}$ tel que $[u]\, T = 0$ pour tout $T \in \mathrm{Tors}(\mathscr{E}(\mathbf{Q}))$ (en fait, il suffit de prendre $u = 8 \times 9 \times 7 \times 5$). Ainsi,

$$\begin{cases} [u]\, \phi_1(P) = [un]\, R \\ [u]\, \phi_2(P) = [um]\, R, \end{cases} \quad \text{et donc,} \quad \begin{cases} \hat{h}(\phi_1(P)) = n^2 \hat{h}(R) \\ \hat{h}(\phi_2(P)) = m^2 \hat{h}(R). \end{cases} \tag{1}$$

De plus, nous savons que [Sil2, Sil3]

$$\begin{cases} \hat{h}(S) = \frac{1}{2} h(S) + O(1) & \forall S \in \mathscr{E}(\mathbf{Q}), \\ h(\phi_i(P)) = d h(P) + O_i(1) & \forall P \in \mathscr{C}(\mathbf{Q}), \qquad i = 1, 2, \end{cases} \tag{2}$$

Les équations (1) et (2) impliquent l'existence d'une constante k (ne dépendant que de $\mathscr{E}$, ϕ_1 et ϕ_2) telle que $|m^2 - n^2| < k$, ce qui nous permet de déduire une borne effective pour les entiers n et m, et donc pour le cardinal de $\mathscr{C}(\mathbf{Q})$.

1.2. *Estimation de* $\hat{h}$

Pour développer de manière explicite les différents résultats du paragraphe précédent, nous allons donner quelques précisions concernant la hauteur canonique $\hat{h}$.

1.2.1. *Différence entre* h *et* $\hat{h}$

Soit $\mathscr{E}$ une courbe elliptique de discriminant Δ et d'invariant modulaire j. J. Silverman a montré le résultat suivant [Sil2]:

$$\forall P \in E(\mathbf{Q}), \qquad -\tfrac{1}{8} h(j) - \tfrac{1}{12} h(\Delta) - 0.973 \leqslant \hat{h}(P) - \tfrac{1}{2} h(P) \leqslant \tfrac{1}{12} h(\Delta) + \tfrac{1}{12} h(j) + 1.07.$$

Dans cet article nous allons travailler exclusivement avec des courbes elliptiques $\mathscr{E}_{a^2}$, d'équation $y^2 = x^3 - a^2 x$, où $a \in \mathbf{Z}_{>0}$ sans facteur carré, pour lesquelles J. Silverman, N. Tzanakis et A. Bremner obtiennent l'encadrement plus fin suivant ([S-T-B]):

Pour tout $P \in \mathscr{E}_{a^2}(\mathbf{Q})$ on a:

$$-\tfrac{1}{2} \log(a) - \tfrac{1}{2} \log(2) \leqslant \hat{h}(P) - \tfrac{1}{2} h(P) \leqslant \tfrac{1}{2} \log(a) + \tfrac{1}{12} \log(2). \tag{3}$$

1.2.2. *Borne inférieure pour* $\hat{h}$

Conjecture [Lan]. Il existe une constante c telle que, pour toute courbe elliptique $\mathscr{E}$ de discriminant minimal Δ, on ait:

$$\forall P \in \mathscr{E}(\mathbf{Q}) \text{ d'ordre infini, } \hat{h}(P) \geqslant c \times \log(\Delta).$$

Ce résultat a été montré par J. Silverman dans le cas des courbes elliptiques dont l'invariant modulaire est entier [Sil4]. Dans le cas particulier des courbes $\mathscr{E}_{a^2}(j(\mathscr{E}_a) = 1728)$, on a [S-T-B]:

$$\hat{h}(P) \geqslant \tfrac{1}{16}\log(2a^2) \qquad \forall P \notin \mathrm{Tors}(\mathscr{E}_{a^2}(\mathbf{Q})) = \{\mathcal{O}, (0,0), (a,0), (-a,0)\}. \quad (4)$$

1.2.3. *Deux résultats importants*

Dans [G-R], G. Grigorov et J. Rizov ont étudié de plus près les courbes $\mathscr{E}_b$ d'équation $y^2 = x^3 - bx$, où $b \in \mathbf{Z}_{>2}$. Ils obtiennent les résultats suivants: Si on pose

$$\Gamma = \{P \in \mathscr{E}_b(\mathbf{Q});\ x(P) = s/t,\ s \geqslant t \geqslant 0,\ \mathrm{pgcd}(s,t) = 1,\ \mathrm{pgcd}(s,b) = 1\}, \text{ on a:}$$

- Pour tout $P \in \Gamma$,

$$\left|\hat{h}(P) - \frac{1}{2}h((P))\right| \leqslant \frac{\log(2)}{2} \text{ (indépendant de } \mathscr{E}_b!) \quad (5)$$

- Si b est sans puissance quatrième, [2] $P \in \Gamma$. (6)

2. DÉTERMINATION DES POINTS RATIONNELS DANS DES FAMILLES DE COURBES DE GENRE 2 ET 3

Dans ce paragraphe, nous allons construire des courbes de genre 2 et 3 comme revêtements de degré 2 de la courbe elliptique $\mathscr{E}_a$. Ces constructions ont été inspirées des travaux de F. Leprévost, E. Howe et B. Poonen [L-H-P] et de ceux de G. Frey et E. Kani [F-K].

2.1. *Courbes de genre* 2

2.1.1. *Construction*

Posons $g(x) = 6(x^2-4)(x^2+2)(x^2+8)$.

PROPOSITION 1. *Soit $a \in \mathbf{Z}_{>0}$ sans facteur carré et soit $\mathscr{C}_a$ la courbe de genre 2 d'équation $ay^2 = g(x)$. Alors il existe deux morphismes ϕ_1 et ϕ_2 de $\mathscr{C}_a$ dans $\mathscr{E}_{a^2}$, indépendants sur* $\mathbf{C}$.

Démonstration. Rappelons que $\mathscr{E}_{a^2}$ a pour équation $y^2 = x^3 - a^2x = f(x)$.

Construisons $\sigma(t) = (c_1t + c_2)/(t + c_3) \in \mathbf{Q}(t)$ tel que σ permute les racines de $f(x)$.

Il suffit de poser $\sigma(t) = -a(t+a)/(3t-a)$ pour obtenir

$$\sigma(0) = a, \qquad \sigma(a) = -a \qquad \text{et} \qquad \sigma(-a) = 0.$$

On a $f(\sigma(t)) = 8a^3t(t+a)(t-a)/(3t-a)^3$ et donc

$$f\left(\sigma\left(\frac{a(x^2+2)}{6}\right)\right) = \frac{8}{27}\,\frac{a^3(x^2+8)(x^2+2)(x^2-4)}{x^6}.$$

Nous obtenons ainsi la courbe $\mathscr{C}_a$ d'équation $ay^2 = g(x) = 6(x^2-4)(x^2+2)(x^2+8)$, qui admet les morphismes:

$$\begin{cases} \phi_1 : \ \mathscr{C}_a \to \mathscr{E}_{a^2} \\ \quad (x, y) \mapsto \left(\dfrac{1}{6}a(2+x^2), \dfrac{1}{36}\,ya^2\right), \\ \phi_2 : \ \mathscr{C}_a \to \mathscr{E}_{a^2} \\ \quad (x, y) \mapsto \left(-\dfrac{1}{3}\,\dfrac{a(8+x^2)}{x^2}, \dfrac{2}{9}\,\dfrac{a^2}{x^3}\right). \end{cases}$$

Comme me l'a suggéré J. Silverman, pour montrer l'indépendance entre ϕ_1 et ϕ_2, nous allons utiliser le résultat suivant [Cas, Lemme 5.]:

Soient $\mathscr{C}$ une courbe algébrique, $\mathscr{A}$ une variété abélienne et $\psi_1, ..., \psi_l$, l morphismes de $\mathscr{C}$ vers $\mathscr{A}$. Alors, si on pose $d(\psi_i, \psi_j) = \frac{1}{2}(d(\psi_i + \psi_j) - d(\psi_i) - d(\psi_j))$, et M la matrice de terme général $d(\psi_i, \psi_j)$ on a:

$$\det(M) \neq 0 \Rightarrow \psi_1, ..., \psi_l \text{ indépendants sur } \mathbf{C}.$$

Un court calcul montre que $d(\phi_1 + \phi_2) = 6$ et $d(2\phi_1) = d(2\phi_2) = 8$ donc, $d(\phi_1, \phi_2) = 2$ et $d(\phi_1, \phi_1) = d(\phi_2, \phi_2) = 4$, d'où la proposition.

COROLLAIRE. *$J(\mathscr{C}_a)$ est isogène à $\mathscr{E}_a \times \mathscr{E}_a$.*

Démonstration. Cf. [C-F, Chap. 14].

2.1.2. *Hauteurs*

PROPOSITION 2. *Pour tout* $P \in \mathscr{C}_a(\mathbf{Q})$ *on a,*

$$\begin{cases} \log\left(\dfrac{3a}{a+3}\right) + 2h(P) \leqslant h(\phi_1(P)) \leqslant \log(3a) + 2h(P) & (7) \\ \log\left(\dfrac{3a}{8a+3}\right) + 2h(P) \leqslant h(\phi_2(P)) \leqslant \log(9a) + 2h(P). & (8) \end{cases}$$

Démonstration. Soit $P = (x, y) \in \mathscr{C}(\mathbf{Q})$, $x = r/s$ avec $(r, s) \in \mathbf{Z} \times \mathbf{Z}_{>0}$. Nous avons:

$$\begin{cases} x(\phi_1(P)) = \dfrac{a(r^2 + 2s^2)}{6s^2} \\ x(\phi_2(P)) = \dfrac{a(r^2 + 8s^2)}{-3r^2}, \end{cases} \quad \text{et donc, si } a \geqslant 2, \quad \begin{cases} h(\phi_1(P)) \leqslant \log(3a) + 2h(P) \\ h(\phi_2(P)) \leqslant \log(9a) + 2h(P). \end{cases}$$

D'autre part,

$$\begin{cases} 3ar^2 = 3 \times (a(r^2 + 2s^2)) + (-a) \times (6s^2) \\ 8as^4 = (6s) \times (a(r^2 + 2s^2)) + (-ar^2) \times (6s^2), \end{cases}$$

$$\Rightarrow \begin{cases} 3ar^4 \leqslant (a+3)\, H(\phi_1(P))\, r^2 \\ 8as^4 \leqslant (a+6)\, H(\phi_1(P)) \max(r^2, s^2) \end{cases}$$

et finalement,

$$\log\left(\frac{3a}{a+3}\right) + 2h(P) \leqslant h(\phi_1(P)) \leqslant \log(3a) + 2h(P).$$

De la même façon, nous obtenons:

$$\log\left(\frac{3a}{8a+3}\right) + 2h(P) \leqslant h(\phi_2(P)) \leqslant \log(9a) + 2h(P), \qquad \text{d'où la proposition.}$$

2.1.3. *Résultats*

Supposons que $\mathscr{E}_{a^2}$ est de rang 1 sur $\mathbf{Q}$ et soit R_a un générateur de la partie libre de $\mathscr{E}_{a^2}(\mathbf{Q})$, nous avons montré au paragraphe 1.1, l'existence, pour tout $P \in \mathscr{C}_a(\mathbf{Q})$ de deux entiers n et m qui vérifient

$$[2]\, \phi_1(P) = [2m]\, R_a \qquad \text{et} \qquad [2]\, \phi_2(P) = [2n]\, R_a.$$

Les équations (1), ..., (3), (7) et (8) nous permettent d'obtenir:

$$|m^2-n^2|<K_a=\frac{72\log(a)+28\log(2)+3\log(3)}{48\hat{h}(R_a)} \tag{9}$$

et comme (4) implique $\hat{h}(R_a)\geqslant 1/16\log(2a^2)$ on a

$$|m^2-n^2|<K'_a=\frac{72\log(a)+28\log(2)+3\log(3)}{6\log(a)+3\log(2)} \tag{10}$$

et alors, si $m\neq\pm n$

$$\min(|m|,|n|)<\frac{K_a-1}{2} \tag{11}$$

$$\min(|m|,|n|)<\frac{K'_a-1}{2}<6. \tag{12}$$

D'autre part, un court calcul montre que:

$$(\phi_1\pm\phi_2)(P)\in\mathrm{Tors}(\mathscr{E}_{a^2}(\mathbf{Q}))$$
$$\Leftrightarrow\begin{cases}P\in\{(\pm 2,0)\} & \text{si}\quad a\neq 6\\ P\in\{(\pm 2,0),(\pm 4,\pm 72),\infty\} & \text{si}\quad a=6.\end{cases}$$

Remarques 1. • Si $P=(x,y)\in\mathscr{C}_a(\mathbf{Q})$ et pour $i=1$ ou 2, $\phi_i(P)=[m]\,R_a+T$ avec $T\in\mathrm{Tors}(\mathscr{E}_{a^2}(\mathbf{Q}))$, alors $\phi_i((x,-y))=-[m]\,R_a+T$. En effet, comme $[2]\,T=0$, on a $-[m]\,R_a+T=-([m]\,R_a+T)$.

• L'inégalité (11) nous permet de déduire que $m\leqslant 5$. Cependant, quand nous aurons à traiter des cas particuliers, la connaissance d'un générateur de $\mathscr{E}_{a^2}(\mathbf{Q})$ nous permettra grâce à (12), d'atteindre des résultats plus précis.

Nous pouvons résumer ce qui précède en le théorème suivant:

THÉORÈME 1. *Si* $\mathscr{E}_{a^2}$ *est de rang* 1 *sur* $\mathbf{Q}$,

$$\textit{le cardinal de } \mathscr{C}_a(\mathbf{Q}) \textit{ est} \leqslant\begin{cases}16\times 5+2=82 & \text{si}\quad a\neq 6,\\ 16\times 5+8=88 & \text{si}\quad a=6.\end{cases}$$

COROLLAIRE. *Si* a *est un nombre premier congru à* 5 *ou* 7 *modulo* 8, *alors la courbe de genre* 2 *d'équation* $ay^2=6(x^2-4)(x^2+2)(x^2+8)$ *possède au plus* 82 *points rationnels.*

Démonstration. Nous savons que si a est un nombre premier congru à 5 ou 7 modulo 8 alors $\mathscr{E}_{a^2}$ est de rang sur $\mathbf{Q}\leqslant 1$ [Kna], d'où le résultat

(en fait, si on admet la conjecture de Birch–Swinnerton-Dyer [B-SD, Kob], $\mathscr{E}_{a^2}$ est de rang exactement 1 sur $\mathbf{Q}$).

EXEMPLE 1. L'arithmétique des courbes elliptiques $\mathscr{E}_{a^2}$ est étroitement liée à l'étude des nombres congruents [Kob, Kna, Ser, Kra, N-W, Tun]. Nous allons utiliser la liste que donne P. Serf de nombres entiers positifs (sans facteur carré) tels que $\mathscr{E}_{a^2}$ est de rang 1 sur $\mathbf{Q}$, et déterminer, grâce à la méthode exposée précédemment, tous les points rationnels de $\mathscr{C}_a$.

Le tableau suivant donne R_a (générateur de la partie libre de $\mathscr{E}_{a^2}(\mathbf{Q})$), K_a (cf. Équation (9)) et $\mathscr{C}_a(\mathbf{Q})$ en fonction de a.

a	R_a	R_a	$\mathscr{C}_a(\mathbf{Q})$
5	$(-4, 6)$	1.3	$\{(\pm 2, 0)\}$
6	$(-2, 8)$	2.27	$\{(\pm 2, 0), (\pm 4, \pm 72), \pm\infty\}$
7	$(25, 120)$	1.06	$\{(\pm 2, 0)\}$
13	$\left(\frac{-36}{25}, \frac{1938}{125}\right)$	0.87	$\{(\pm 2, 0)\}$
14	$\left(\frac{-7}{4}, \frac{147}{8}\right)$	1.54	$\{(\pm 2, 0)\}$
15	$(-9, 36)$	2.02	$\{(\pm 2, 0)\}$
22	$\left(\frac{-2}{9}, \frac{280}{27}\right)$	1.1	$\{(\pm 2, 0)\}$
23	$\left(\frac{42025}{289}, \frac{8506680}{4913}\right)$	0.5	$\{(\pm 2, 0)\}$

Nous allons voir qu'il est possible d'améliorer nettement ces derniers résultats en procédant de manière analogue à [G-R, Théorème 1.5.].

THÉORÈME 2. *Pour tout* $a \neq 6 \in \mathbf{Z}_{>0}$ *tel que* $\operatorname{rang}(\mathscr{E}_{a^2}) = 1$ *sur* $\mathbf{Q}$, $\mathscr{C}_a(\mathbf{Q}) = \{(\pm 2, 0)\}$.

Démonstration. Nous savons que si $S = (u, v) \in \mathscr{E}_{a^2}$, alors $x([2]S) = (u^2 + a^2)^2/4v^2$ et donc, pour tout $P = (x/z, y/z) \in \mathscr{C}_a$ (avec $\operatorname{pgcd}(x, y, z) = 1$) nous obtenons:

$$\begin{cases} x([2]\,\phi_1(P)) = \dfrac{(40z^4 + 4z^2x^2 + x^4)^2}{4z^6y^2} \\ x([2]\,\phi_2(P)) = \dfrac{(32z^4 + 8z^2x^2 + 5x^4)^2}{4z^4x^2y^2}. \end{cases}$$

Il est facile de remarquer que les seuls diviseurs communs de $(40z^4+4z^2x^2+x^4)^2$ et $4z^6y^2$ sont 2 et 3 et, si on regarde de plus près on trouve:

$$\operatorname{pgcd}((40z^4+4z^2x^2+x^4)^2, 4z^6y^2) = (\operatorname{pgcd}(8, x^4)\operatorname{pgcd}(3, y))^2.$$

Par un raisonnement analogue nous obtenons:

$$\operatorname{pgcd}((32z^4+8z^2x^2+5x^4)^2, 4z^4x^2y^2) = (\operatorname{pgcd}(32, x^4)\operatorname{pgcd}(3, y))^2 \operatorname{pgcd}(5, z)^2.$$

Ainsi,

$$\begin{cases} h([2]\,\phi_1(P)) = 2\log\left(\dfrac{40z^4+4z^2x^2+x^4}{\operatorname{pgcd}(8, x^4)\operatorname{pgcd}(3, y)}\right) \\ h([2]\,\phi_2(P)) = 2\log\left(\dfrac{32z^4+8z^2x^2+5x^4}{\operatorname{pgcd}(32, x^4)\operatorname{pgcd}(3, y)\operatorname{pgcd}(5, z)}\right) \end{cases}$$

$$\Rightarrow \begin{cases} |h([2]\,\phi_1(P)) - h([2]\,\phi_2(P))| \\ \qquad \leqslant 2\left|\log\left(\dfrac{40z^4+4z^2x^2+x^4}{32z^4+8z^2x^2+5x^4}\right)\right| + 2\left|\log\left(\dfrac{\operatorname{pgcd}(8, x^4)}{\operatorname{pgcd}(32, x^4)\operatorname{pgcd}(5, z)}\right)\right| \\ \qquad \leqslant 2\log(5.2) + 2\log 20 = 2\log(104). \end{cases}$$

Par ailleurs, (5) et (6) impliquent:

$$\begin{cases} |\hat{h}([2]\,\phi_1(P)) - \hat{h}([2]\,\phi_2(P))| \\ \qquad \leqslant |\hat{h}([2]\,\phi_1(P)) - \tfrac{1}{2}h([2]\,\phi_1(P))| + |\hat{h}([2]\,\phi_2(P)) - \tfrac{1}{2}h([2]\,\phi_2(P))| \\ \qquad\quad + \tfrac{1}{2}\,|h([2]\,\phi_1(P)) - h([2]\,\phi_2(P))| \\ \qquad \leqslant \log 2 + \log 104 = \log 208. \end{cases}$$

En remarquant que pour tout $S \in \mathscr{E}_{a^2}$ $\hat{h}([2]\,S) = 4\hat{h}(S)$, nous obtenons:

$$|\hat{h}(\phi_1(P)) - \hat{h}(\phi_2(P))| \leqslant \frac{\log 208}{4}. \tag{13}$$

Comme dans le paragraphe 1, pour tout $P \in \mathscr{C}(\mathbf{Q})$, il existe par construction, des entiers n et m et des points T_1, T_2 dans $\operatorname{Tors}(\mathscr{E}_{a^2}(\mathbf{Q}))$ tels que

$$\begin{cases} \phi_1(P) = [n]\,R + T_1 \\ \phi_2(P) = [m]\,R + T_2. \end{cases}$$

De (1) et (13) nous pouvons conclure: $\min(m, n) \leqslant (2\log 208/\log(2a^2)) - 1/2 \Rightarrow \min(m, n) < 1$ dès que $a \geqslant 25$. Le cas où $a \leqslant 24$ ayant été traité dans l'exemple 1, le théorème s'ensuit.

2.2. *Courbes de Genre* 3

2.2.1. *Construction*

Posons $h(x) = -x(x-1)(x+1)(x+2)(2x+1)(1+x+x^2)$.

PROPOSITION 3. *Soit $a \in \mathbf{Z}_{>0}$ sans facteur carré et $\mathscr{D}_a$ la courbe de genre 3 d'équation $ay^2 = h(x)$. Alors, il existe deux morphismes ϕ_1 et ϕ_2 de $\mathscr{D}_a$ dans $\mathscr{E}_{a^2}$, indépendants sur* **C**.

Démonstration. Si x et z vérifient $f(z) = f(w)$ (où $f(x) = x^3 - a^2x$) et $z \neq w$, alors il est facile de voir que (z, w) est un point de la conique $\mathscr{D}_0$: $z^2 + wz + w^2 = a^2$.

$\mathscr{D}_0$ passe par le point rationnel $(0, p)$ et admet donc la paramétrisation suivante:

$$\begin{cases} z(x) = \dfrac{a(2x+1)}{1+x+x^2} \\ w(x) = \dfrac{a(x-1)(x+1)}{1+x+x^2}. \end{cases}$$

Soit $\mathscr{D}_a$ la courbe de genre 3 d'équation

$$\begin{aligned} ay^2 &= \frac{1}{a^3} f(z(x))(1+x+x^2)^4 \\ &= -x(x-1)(x+1)(x+2)(2x+1)(1+x+x^2) \\ &= h(x). \end{aligned}$$

Nous avons les morphismes suivants de $\mathscr{D}_a$ vers $\mathscr{E}_{a^2}$:

$$\begin{cases} \phi_1 : \quad \mathscr{D}_a \to \mathscr{E}_{a^2} \\ (t, s) \mapsto \left(z(x), \dfrac{a^2 y}{(1+x+x^2)^2} \right), \\ \phi_2 \quad : \mathscr{D}_a \to \mathscr{E}_{a^2} \\ (t, s) \mapsto \left(w(x), \dfrac{a^2 y}{(1+x+x^2)^2} \right). \end{cases}$$

Il est facile de vérifier—par la même méthode que dans la Proposition 1—que ϕ_1 et ϕ_2 sont indépendants sur **C**.

COROLLAIRE. *Il existe une courbe elliptique $\mathscr{E}'_{a^2}$ définie sur* **Q** *telle que $\mathscr{J}(\mathscr{D}_a)$ est isogène à $\mathscr{E}_{a^2} \times \mathscr{E}_{a^2} \times \mathscr{E}'_{a^2}$.*

Démonstration. Il suffit de montrer que les formes différentielles $\phi_1^*(dx_1/y_1)$, $\phi_2^*(dx_2/y_2)$ sont linéairement indépendantes.

Nous obtenons:

$$\begin{cases}\phi_1^*(dx_1/y_1) = 1/a(-x^2-4x-1)(dx/y),\\ \phi_2^*(dx_2/y_2) = 1/a(-x^2+2x+2)(dx/y).\end{cases}$$

Quand nous écrivons $\phi_1^*(dx_1/y_1)$ et $\phi_2^*(dx_2/y_2)$ dans la base dx/y, $x\,dx/y$, $x^2\,dx/y$ nous obtenons la matrice

$$\begin{bmatrix} -1/a & -4/a & -1/a \\ -1/a & 2/a & 2/a \end{bmatrix},$$

qui est de rang 2, d'où le corollaire.

2.2.2. *Hauteurs*

PROPOSITION 4. *Pour tout* $P \in \mathscr{D}_a(\mathbf{Q})$ *on a,*

$$\begin{cases}\log\left(\dfrac{3a}{4a+3}\right) + 2h(P) \leqslant h(\phi_1(P)) \leqslant \log(3a) + 2h(P) & (14)\\[2ex] \log\left(\dfrac{3a}{3a+2}\right) + 2h(P) \leqslant h(\phi_2(P)) \leqslant \log(3a) + 2h(P). & (15)\end{cases}$$

Démonstration. Soit $P=(x,\,y)\in\mathscr{D}_a(\mathbf{Q})$, $x=r/s$ avec $(r,\,s)\in\mathbf{Z}\times\mathbf{Z}_{>0}$. Nous avons:

$$\begin{cases} x(\phi_1(P)) = \dfrac{a(s^2+2rs)}{r^2+rs+s^2}\\[2ex] x(\phi_2(P)) = \dfrac{a(r^2-s^2)}{r^2+rs+s^2}, \qquad \text{et donc,}\end{cases}$$

$$\begin{cases} h(\phi_1(P)) \leqslant \log(3a) + 2h(P)\\ h(\phi_2(P)) \leqslant \log(3a) + 2h(P).\end{cases}$$

D'autre part,

$$\begin{cases} 3as^3 = (-s-2r)\times(a(s^2+2rs)) + (4as)\times(r^2+rs+s^2)\\ 3ar^3 = (-s-2r)\times(a(s^2+2rs)) + (as+3ar)\times(r^2+rs+s^2),\end{cases}$$

$$\Rightarrow \begin{cases} 3as^3 \leqslant (4a+3)\,H(\phi_1(P))\max(|r|,\,|s|)\\ 3ar^3 \leqslant (4a+3)\,H(\phi_1(P))\max(|r|,\,|s|),\end{cases}$$

et finalement,

$$\log\left(\frac{3a}{4a+3}\right)+2h(P)\leqslant h(\phi_1(P))\leqslant\log(3a)+2h(P).$$

De la même façon nous obtenons:

$$\log\left(\frac{3a}{3a+2}\right)+2h(P)\leqslant h(\phi_2(P))$$

$$\leqslant\log(3a)+2h(P), \qquad \text{d'où la proposition.}$$

2.2.3. *Résultats*

Supposons que $\mathscr{E}_{a^2}$ soit de rang 1 sur $\mathbf{Q}$ et soit R_a un générateur de la partie libre de $\mathscr{E}_{a^2}(\mathbf{Q})$, nous avons montré au paragraphe 1.1, l'existence, pour tout $P\in\mathscr{D}_a(\mathbf{Q})$ de deux entiers n et m qui vérifient

$$[2]\,\phi_1(P)=[2m]\,R_a \qquad \text{et} \qquad [2]\,\phi_2(P)=[2n]\,R_a.$$

Les équations (1), ..., (3), (14) et (15) nous permettent d'obtenir:

$$|m^2-n^2|<K_a=\frac{72\log(a)+24\log(5)+21\log(2)}{48\hat{h}(R_a)} \tag{16}$$

et comme (4) implique $\hat{h}(R_a)\geqslant 1/16\log(2a^2)$ on a

$$|m^2-n^2|<K'_a=\frac{72\log(a)+24\log(5)+21\log(2)}{6\log(a)+3\log(2)} \tag{17}$$

et alors, si $m\neq\pm n$,

$$\begin{cases}\min(|m|,|n|)<\dfrac{K_a-1}{2} & (18)\\[2ex] \min(|m|,|n|)<\dfrac{K'_a-1}{2}<6. & (19)\end{cases}$$

D'autre part, un court calcul montre que:

$$(\phi_1\pm\phi_2)(P)\in\mathrm{Tors}(\mathscr{E}(\mathbf{Q}))$$

$$\Leftrightarrow P\in\{(0,0),(1,0),(-1,0),(-2,0),(-1/2,0)\}.$$

Remarques 2. • Comme dans le cas du genre 2, si $P=(x, y)\in\mathscr{D}_a(\mathbf{Q})$ et pour $i=1$ ou 2, $\phi_i(P)=[m]\,R_a+T$ où $T\in\mathrm{Tors}(\mathscr{E}(\mathbf{Q}))$, alors $\phi_i((x, -y))=-[m]\,R_a+T$.

• L'inégalité (19) nous permet de déduire que $m\leqslant 5$.

Nous pouvons résumer ce qui précède en le théorème suivant:

THÉORÈME 3. *Si* $\mathscr{E}_{a^2}$ *est de rang* 1 *sur* $\mathbf{Q}$,

$$\text{le cardinal de } \mathscr{D}_a(\mathbf{Q}) \text{ est } \leqslant 16\times 5+5=85.$$

COROLLAIRE. *Si* a *est un nombre premier congru à* 5 *ou* 7 *modulo* 8, *alors la courbe de genre* 3 *d'équation* $ay^2=-x(x-1)(x+1)(x+2)(2x+1)(1+x+x^2)$ *possède au plus* 85 *points rationnels.*

Démonstration. Analogue au cas des courbes de genre 2.

EXEMPLE 2. Le tableau suivant donne, comme dans le cas des courbes de genre 2, R_a et K_a (cf. équation (13)) et $\mathscr{D}_a(\mathbf{Q})$ en fonction de l'entier a.

a	R_a	K_a	$\mathscr{D}_a(\mathbf{Q})$
5	$(-4, 6)$		$\{(0, 0), (1, 0), (-1, 0), (-2, 0), (-1/2, 0)\}$
6	$(-2, 8)$		$\{(0, 0), (1, 0), (-1, 0), (-2, 0), (-1/2, 0)\}$
7	$(25, 120)$		$\{(0, 0), (1, 0), (-1, 0), (-2, 0), (-1/2, 0)\}$

Dans ce cas il est aussi possible d'améliorer nettement ces derniers résultats en considérant (5) et (6).

THÉORÈME 4. *Pour tout* $a\in\mathbf{Z}_{>0}$ *tel que* $\mathrm{rang}(\mathscr{E}_{a^2})=1$ *sur* $\mathbf{Q}$,

$$\mathscr{D}_a(\mathbf{Q})=\{(0, 0), (1, 0), (-1, 0), (-2, 0), (-1/2, 0)\}.$$

Démonstration. On a:

$$\begin{cases} x([2]\,\phi_1(P))=\dfrac{(7x^2z^2+6xz^3+2zx^3+x^4)^2}{4z^6y^2} \\ x([2]\,\phi_2(P))=\dfrac{(2x^4+x^2z^2+2+2xz^3+2zx^3)^2}{4z^6y^2}. \end{cases}$$

Il est facile de remarquer que les seuls diviseurs communs de $(7x^2z^2 + 6xz^3 + 2zx^3 + x^4)^2$ et $4z^6y^2$ sont 2 et 3 et, si on regarde de plus près on trouve

$$\operatorname{pgcd}((7x^2z^2 + 6xz^3 + 2zx^3 + x^4)^2, 4z^6y^2) = (\operatorname{pgcd}(2, x) \operatorname{pgcd}(3, y))^2.$$

Par un raisonnement analogue nous obtenons:

$$\begin{aligned}\operatorname{pgcd}((2x^4 + x^2z^2 + 2 + 2xz^3 + 2zx^3)^2, 4z^6y^2)\\ = (\operatorname{pgcd}(2, x) \operatorname{pgcd}(2, z) \operatorname{pgcd}(3, y))^2.\end{aligned}$$

Ainsi,

$$\begin{cases} h([2]\,\phi_1(P)) = 2\log\left(\dfrac{7x^2z^2 + 6xz^3 + 2zx^3 + x^4}{\operatorname{pgcd}(2, x) \operatorname{pgcd}(3, y)}\right) \\ h([2]\,\phi_2(P)) = 2\log\left(\dfrac{2x^4 + x^2z^2 + 2 + 2xz^3 + 2zx^3}{\operatorname{pgcd}(2, x) \operatorname{pgcd}(2, z) \operatorname{pgcd}(3, y)}\right) \end{cases}$$

$$\Rightarrow \begin{cases} |h([2]\,\phi_1(P)) - h([2]\,\phi_2(P))| \\ \qquad \leqslant 2\left|\log\left(\dfrac{7x^2z^2 + 6xz^3 + 2zx^3 + x^4}{2x^4 + x^2z^2 + 2 + 2xz^3 + 2zx^3}\right)\right| + 2\ |\log 2| \\ \qquad \leqslant 2\log(2.01) + 2\log 2 = 2\log(4.02). \end{cases}$$

Par ailleurs, (5) et (6) impliquent:

$$\begin{cases} |\hat{h}([2]\,\phi_1(P)) - \hat{h}([2]\,\phi_2(P))| \\ \quad \leqslant |\hat{h}([2]\,\phi_1(P)) - \frac{1}{2}h([2]\,\phi_1(P))| + |\hat{h}([2]\,\phi_2(P)) - \frac{1}{2}h([2]\,\phi_2(P))| \\ \qquad + \frac{1}{2}\,|h([2]\,\phi_1(P)) - h([2]\,\phi_2(P))| \\ \quad \leqslant \log 2 + 2\log 4.01. \end{cases}$$

En remarquant que pour tout $S \in \mathscr{E}_{a^2}$, $\hat{h}([2]\,S) = 4\hat{h}(S)$, nous obtenons:

$$|\hat{h}(\phi_1(P)) - \hat{h}(\phi_2(P))| \leqslant \frac{\log 2 + 2\log 4.01}{4}. \tag{20}$$

Comme dans les préliminaires, pour tout $P \in \mathscr{C}(\mathbf{Q})$, il existe par construction, des entiers n et m et des points T_1, T_2 dans $\operatorname{Tors}(\mathscr{E}_{a^2}(\mathbf{Q}))$ tels que:

$$\begin{cases} \phi_1(P) = [n]\,R + T_1 \\ \phi_2(P) = [m]\,R + T_2. \end{cases}$$

De (1) et (20) nous pouvons conclure:

$$\min(m, n) \leqslant \frac{2\log 2 + 4\log 4.01}{\log(2a^2)} - \frac{1}{2} \Rightarrow \min(m, n) < 1 \qquad \text{dès que } a \geqslant 8.$$

Le cas où $a \leqslant 7$ ayant été traité dans l'exemple 2, le théorème s'ensuit.

RÉFÉRENCES

[Bom] E. Bombieri, The Mordell conjecture revisited, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **17**, No. 4 (1990), 615–640.

[Bru] N. Bruin, The diophantine equations: $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, preprint.

[B-SD] B. J. Birch et H. P. F. Swinnerton-Dyer, Notes on elliptic curves, I and II, *J. Reine Angew. Math.* **212–218** (1963–1965).

[Cas] J. W. S. Cassels, On a theorem of Dem'janenko, *J. London Math. Soc.* **43** (1968), 61–66.

[C-F] J. W. S. Cassels et E. V. Flynn, "Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2," London Math. Soc. Lectures Note Ser., Vol. 230, Cambridge Univ. Press, Cambridge, UK, 1996.

[Cha] C. Chabauty, Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension, *C. R. Acad. Sci. Paris* **212** (1941), 1022–1024.

[Col] R. F. Coleman, Effective Chabauty, *Duke Math. J.* **52** (1985), 765–770.

[Dem] V. Dem'janenko, Rational points of a class of algebraic curves, *in* "Amer. Math. Soc. Transl.," Vol. 66, pp. 246–272, Amer. Math. Soc., Providence, 1968.

[Fal1] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern (Finiteness theorems for abelian varieties over number fields), *Invent. Math.* **73**, No. 3 (1983), 349–366. [In German]

[Fal2] G. Faltings, Diophantine approximation on abelian varieties, *Ann. of Math. (2)* **133**, No. 3 (1991), 549–576.

[Flyn] E. V. Flynn, A flexible method for applying Chabauty's theorem, *Compositio Math.* **105** (1997), 79–94.

[F-P-S] E. V. Flynn, B. Poonen, et E. F. Schaefer, Cycles of quadratic polynomials and rational points on a genus-2 curve, *Duke Math. J.* **90**, No. 3 (1997), 435–463.

[F-K] G. Frey et E. Kani, Curves of genus 2 covering elliptic curves and an arithmetical application, *in* "Arithmetic Algebraic Geometry (Texel, 1989)" Progr. Math., Vol. 89, pp. 153–176, Birkhäuser, Boston, 1991.

[G-G] D. M. Gordon et D. Grant, Computing the Mordel–Weil rank of Jacobians of curves of genus two, *Trans. Amer. Math. Soc.* **337**, No. 2 (1993), 807–824.

[G-R] G. Grigorov et J. Rizov, Heights on elliptic curves and the equation $x^4 + y^4 = cz^4$, preprint.

[Kna] A. Knapp, "Elliptic Curves," Math. Notes, Princeton Univ. Press, Princeton, NJ, 1992.

[Kob] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms," Springer-Verlag, New York/Berlin, 1984.

[Kra] G. Kramarz, All congruent numbers less than 2000, *Math. Ann.* **273**, No. 2 (1986), 337–340.

[Lan] S. Lang, "Elliptic Curves: Diophantine Analysis," Grundlehren der Mathematischen Wissenschaften, Vol. 231, Springer-Verlag, Berlin, 1978.

[L-H-P] F. Leprévost, E. Howe, et B. Poonen, Sous-groupes de torsion d'ordres élevés de jacobiennes décomposables de courbes de genre 2 (Large torsion subgroups of split Jacobians of curves of genus 2), *C. R. Acad. Sci. Paris Sér. I Math.* **323**, No. 9 (1996), 1031–1034. [In French]

[Man] Y. Manin, The p-torsion of elliptic curves is uniformly bounded, *Izv. Akad. Nauk SSSR* **33** (1969), 459–465. [In Russian]

[Maz] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–169.

[N-W] K. Noda et H. Wada, All congruent numbers less than 10 000, *Proc. Japan Acad. Ser. A Math. Sci.* **69**, No. 6 (1993), 175–178.

[Ser] P. Serf, Congruent numbers and elliptic curves, *in* "Computational Number Theory (Debrecen, 1989)," pp. 227–238, de Gruyter, Berlin, 1991.

[Serre] J.-P. Serre, "Lecture on Mordel–Weil Theorem," Vieweg, Wiesbaden, 1989.

[Sik] S. Siksek, On Serre's equation: $x^4 + y^4 = 17$, preprint, 1997.

[Sil1] J. H. Silverman, Rational points on certain families of curves of genus at least 2, *Proc. London Math. Soc. (3)* **55** (1987), 465–481.

[Sil2] J. H. Silverman, The arithmetic of elliptic curves, *in* "Graduate Texts in Mathematics," Vol. 106, Springer-Verlag, New York/Berlin, 1986.

[Sil3] J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **55**, No. 192 (1990), 723–743.

[Sil4] J. H. Silverman, Lower bound for the canonical height on elliptic curves, *Duke Math. J.* **48**, No. 3 (1981), 633–648.

[S-T-B] J. H. Silverman, N. Tzanakis, et A. Bremner, Integral points in arithmetic progession on $y^2 = x(x^2 - n^2)$, preprint.

[Tun] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.* **72**, No. 2 (1983), 323–324.

[Voj] Vojta, Paul Siegel's theorem in the compact case, *Ann. of Math. (2)* **133**, No. 3 (1991), 509–548.

[Wet] J. L. Wetherell, "Bounding the number of rational points on certain curves of high rank," Ph.D. dissertation, Berkeley, 1997.